UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/775,797 | 02/10/2004 | Ramarathnam Venkatesan | MS307073.01/MSFTP588US | 9675 |

27195 7590 02/15/2008

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

| EXAMINER | |
|---|---|
| TRAORE, FATOUMATA | |
| **ART UNIT** | **PAPER NUMBER** |
| 2136 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 02/15/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
osteuball@thepatentattorneys.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/775,797 | VENKATESAN ET AL. | |
| | Examiner | Art Unit | |
| | Fatoumata Traore | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-4 and 6-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This is in response to the RCE filed October 31, 2007. Claims 1, 6, 9-11, 20, 28 and 33-35 have been amended; Claim 5 has been cancelled; Claims 1-35 are pending and have been considered below.

### *Claim Rejections - 35 USC § 101*

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 1 is drawn to components, which the applicant has defined in the specification (page 7, lines 4-15) to encompass a program, an executable, etc). A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine or manufacture. A computer program is not a combination of substances and therefore not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention. Therefore, Claim 1 and dependant claims 2-19 are not statutory.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 11, 12, 20, 26-28, 31, and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Manferdelli et al (US 7,051,200) in view of Holtaus et al (US 6, 229,897).

***Claims 1, 20, 28 and 33-35***: Manferdelli et al discloses a system, a method and a computer readable medium of software protection using random code generation, comprising:

i. A component that receives a first code designed in a noise model, the first code comprises algorithms utilized to correct noise errors with high probability, the first code is intended to refer to encoded data as well as error detection codes and includes a linear code *(error correction principles are employed to correct errors brought about noise during data transmission)(column 13, line 60 to column 14, lines 35)*; and

ii. a transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, the transformation component utilizes a random number generator to perform algebraic transformations on data utilizing the first code to generate the new code, and the transformation component hides the first code via randomizing data that employs the first code thereby not enabling the computationally bounded adversary to determine a location of critical bits to attack *(column 14, line 36 to column 15, lines 15)*, wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code

by the computationally bounded adversary would appear as a noise attack on the first code*(column 14, line 36 to column 15, lines 15)*; and

wherein the first code designed in the noise model utilizes the algorithms to correct the noise errors with a high success rate*(column 14, line 36 to column 15, lines 15)*; and

but does not explicitly indicate that wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code nor a decoder that determines the first code from the new code, the decoder accesses algorithms utilized by the transformation component to decode the new code and determine the first code.

However, Holthaus et al discloses a system of secured analog voice communication, which further discloses:

i. Wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code (column 5, lines 44-52);

ii. A decoder (*descrambler*) that determines the first code from the new code, the decoder accesses algorithms utilized by the transformation component to decode the new code and determine the first code (column5, lines 30-45; line 65 to column 6, line 10).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al such to determine the first code from the first code. One would have been motivated to do so in order to provide to provide an improvement to analog scrambling where a higher level of security can be achieved (column 2, lnes37-40).

***Claim 2***: Manferdelli et al and Holthaus et al disclose a system as in claim 1 above and Manferdelli et al further discloses that the new code the new code appears random to the computationally bounded adversary *(column 9, lines 28-62)*.

***Claim 3***: Manferdelli et al and Holthaus et al disclose a system as in claim 1 above and Manferdelli et al further discloses that an adversarial attack by the bounded adversary on the new code is randomly distributed on the first code *(column 9, lines 28-62)*..

***Claim 4***: Manferdelli et al and Holthaus et al disclose a system as in claim 1 above and Manferdelli et al further discloses that the transformation component comprises a pseudo-random number generator that facilitates transforming the first code into the new code(Fig. 4, item 404).

***Claim 11***: Manferdelli et al and Holthaus et al disclose a system as in claim 1 above and Manferdelli et al further discloses wherein the first code is generated based at least in part on a sequence of messages (Fig. 7).

***Claims 12 and 31***: Manferdelli et al and Holthaus et al disclose a system as in claims 1 and 28 above, and Holthaus et al further discloses that the decoder knowing the sequence of messages (column 5, lines 38-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Manferdelli et al such to include a sequence of message. One would have been motivated to do so in order to provide to provide an improvement to analog scrambling where a higher level of security can be achieved (column 2, lines 37-40).

***Claims 26 and 27***: Manferdelli et al and Holthaus et al disclose a system as in claim 1 above, Holthaus et al furter discloses that the code hiding module embeds synchronization information into the second code (column 5, lines 44-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Manferdelli et al such to embed synchronization information into the code. One would have been motivated to do so in order to provide to provide an improvement to analog scrambling where a higher level of security can be achieved (column 2, lines 37-40).

5. Claims 13-19, 30 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Manferdelli et al (US 7,051,200) in view of Holtaus et al (US 6, 229,897) in further view of Venkatsesan et al (US 6,829,710).

***Claims 13 and 17***: Manferdelli et al and Holthaus et al disclose a system as in claims 12 above and 16 below, while neither of them indicate and Manferdelli et al further discloses a pseudo random number generator, while neither of them indicate that the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and generating a random permutation σ that permutes the n bits. However, Venkatesan et al discloses a technique for producing, through watermarking, which further discloses that the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and generating a random permutation σ that permutes the n bits(Fig. 9A, item 936).Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

***Claim 14:*** Manferdelli et al, Holthaus et al and Venkatesan et al disclose a system as in claim 13 above, and Venkatesan et al further discloses the transformation component sends a randomized code word to the decoder, the randomized code word having the form a x ~(f(mi ))+ b, wheref is an encoding function, m is a message, i is the position of the message within the sequence, and x is a bitwise multiplication operator(column 8, lines 34-43). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

***Claims 15 and 30:*** Manferdelli et al, Holthaus et al and Venkatesan et al disclose a system as in claims 11 and 28 above, and Venkatesan et al further discloses that the transformation component embeds information relating to the sequence of messages into the new code (column 7, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

***Claim 16:*** Manferdelli et al, Holthaus et al and Venkatesan et al disclose a system as in claim 15 above, and Venkatesan et al further discloses that the first code has a length of nl, and the information relating to the sequence of messages embedded in nl locations in the new code(column 7, lines 1-51). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

***Claim 18:*** Manferdelli et al, Holthaus et al and Venkatesan et al disclose a system as in claim 17 above, and Venkatesan et al further discloses that an

encoder sending the new code to the decoder, the new code having embedded therein the seed (column 8, lines 10-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

***Claim 19:*** Manferdelli et al, Holthaus et al and Venkatesan et al disclose a system as in claim 1 above, and Venkatesan et al further discloses that the first code including information relating to authorization of use of the first code, and further comprising a tracing component that determines whether a user is authorized to use the first code (column 3, lines 24-30). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

***Claim 32***: Manferdelli et al and Holthaus et al disclose a system as in claim 31 above, while neither of them indicate and Manferdelli et al further discloses a pseudo random number generator, while neither of them indicate that the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and generating a random permutation $\sigma$ that permutes the n bits. However, Venkatesan et al discloses a technique for producing, through

watermarking, which further discloses that the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and generating a random permutation σ that permutes the n bits (Fig. 9A, item 936),and embedding the seed into the first code (column 8, lines 10-35).Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to generate two random numbers. One would have been motivated to securely watermark any executable (cloumn4, lines4-49).

6. Claims 6-8 and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Manferdelli et al (US 7,051,200) in view of Holtaus et al (US 6, 229,897) in further view of Cox et at (US 6,275,965).

***Claim 6***: Manferdelli et al and Holthaus et al disclose a system as in claim 1 above, while neither of them explicitly discloses that the decoder comprising a checking component that determines whether the first code has been corrupted. However, Cox et al discloses a system for efficient error detection and correction, which further discloses that the decoder comprising a checking component that determines whether the first code has been corrupted *(column 8, lines 10-23)*. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to include a checking component in the decoder.

One would have been motivated to do so in order to provide for enhancing the error detection and correction capability obtained when a plurality of data byte strings or vectors are interleaved and encoded in a two-level, block-formatted linear code using codeword (subblock) and block-level redundancy (column 2, line 64 to column 3, line 2).

***Claim 7***: Manferdelli et al , Holthaus et al and Cox et al disclose a system as in claim 6 above, Cox et al further discloses a system for efficient error detection and correction, which further discloses that the the checking component utilizing a checking function h" Zn ~ {0,1}, where E is a finite alphabet that defines a family of codes and n is a length parameter for E (column 11, line 66 to column 12, line 40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to use checking function. One would have been motivated to do so in order to provide for enhancing the error detection and correction capability obtained when a plurality of data byte strings or vectors are interleaved and encoded in a two-level, block-formatted linear code using codeword (subblock) and block-level redundancy (column 2, lne 64 to column 3, line 2).

***Claim 8***: Manferdelli et al , Holthaus et al and Cox et al disclose a system as in claim 6 above, and Cox et al discloses further discloses that the checking component outputting a vector, the first code being corrupted when the vector is a non-zero vector (column 8, lines 23-38, column 9, line9-25; Fig. 5). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Manferdelli et al and Holthaus et al such to compute a nonzero vector output. One would have been motivated to do so in order to provide for enhancing the error detection and correction capability obtained when a plurality of data byte strings or vectors are interleaved and encoded in a two-level, block-formatted linear code using codeword (subblock) and block-level redundancy (column 2, lne 64 to column 3, line 2).

***Claims 25 and 29***: Manferdelli et al and Holthaus et al disclose a system as in claims 20 and 28 above, while neither of them explicitly discloses that comprising decoding the message, wherein the message is decoded at least in part by solving a minimum vertex cover problem. However, Cox et al discloses a system for efficient error detection and correction, which further discloses that comprising decoding the message, wherein the message is decoded at least in part by solving a minimum vertex cover problem(column 3, line 50 to column 4, lines 15). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al such as to solve a vertex problem. One would have been motivated to do so in order to increase data integrity and system security.

7. Claims 9 and10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Manferdelli et al (US 7,051,200) in view of Holtaus et al (US 6, 229,897) in further view

of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658- 667, ISBN: 0-7695-1116-3)

***Claim 9***: Manferdelli et al and Holthaus et al disclose a system as in claim 5 above, while neither reference explicitly discloses that the decoder utilizes a unique decoding function, Manferdelli et al and Holthaus et al discloses a similar system, which further discloses a decoder utilizing a unique decoding function (we further consider the list decoding version) (introduction and section 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al such as to include a unique decoding function. One would have been motivated to do so in order to increase data integrity and system security.

***Claim 10***: Manferdelli et al and Holthaus et al disclose a system as in claim 5 above. While neither reference explicitly discloses that the decoder utilizes a list decoding function g, Guruswami discloses a similar system, which further discloses a decoder utilizing a list decoding function (we further consider the list decoding version) (introduction and section 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al such as to include a list decoding function. One would have been motivated to do so in order to increase data and system security.

8. Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Manferdelli et al (US 7,051,200) in view of Holtaus et al (US 6, 229,897) in further view of Bohnke (US 6,557,139).

***Claim 21***: Manferdelli et al and Holthaus et al disclose a system as in claim 20 above, while neither of them explicitly discloses that the message is encoded with a minimum relative distance. However, Bohnke discloses a similar system, which further discloses an encoding component that encodes a message and creates a code word, the encoding component encodes the message with a code that has a minimum relative distance. Epsilon. And rate 1-.kappa..epsilon. for some constant .kappa.>1. (In FIG. 3, a block diagram of an encoding structure according to the present invention is shown, which comprises a data input means, a checksum generator, a frame formatter and a turbo encoder. The data input means receives serially arranged data bits, e. g. in data frames consisting of N data bits, d.sub.0, d.sub.1, . . . d.sub.N-1. (Column 5, lines 50-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al such as to include such an encoder. One would have been motivated to do so in order to increase data and system security.

***Claim 22***: Manferdelli et al and Holthaus et al, and Bohnke disclose a system as in claim 21 above, and Bohnke further discloses a component that utilizes the encoded message and divides the encoded message into a number of blocks B, the B blocks being of substantially similar size (Fig.1). Therefore, it would have

been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al such as to use block encryption. One would have been motivated to do so in order to increase data and system security

***Claim 23***: Manferdelli et al and Holthaus et al, and Bohnke disclose a system as in claim 22 above, and Bohnke further discloses the plurality of blocks encoded using (n, k, n – k + 1) Reed-Solomon code, where n is a resulting size of the encoded blocks and k is a size of the blocks prior to encoding (column 7, lines 25-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al such as to use the Reed-Solomon code. One would have been motivated to do so in order to increase data and system security.

9. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Manferdelli et al (US 7,051,200) in view of Holtaus et al (US 6, 229,897) and Bohnke (US 6,557,139) in further view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658- 667, ISBN: 0-7695-1116-3)

***Claim 24***: Manferdelli et al and Holthaus et al, and Bohnke disclose a system as in claim 23 above. While neither reference explicitly discloses that the code hiding module comprising a bipartite expander graph with a number of edges being substantially similar to Bn, and symbols within the B blocks are randomly

assigned an edge within the bipartite expander graph, Guruswami discloses a similar system, which further discloses an expander graph with a number of edges being substantially similar to Bn, and symbols within the B blocks are randomly assigned an edge within the bipartite expander graph(the construction employ expander graphs, which facilitate efficient decoding algorithms through various forms of voting procedures) (introduction and section 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined method of Manferdelli et al and Holthaus et al, and Bohnke such as to include an expander graph. One would have been motivated to do so in order to increase data and system security.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Monday, February 11, 2008

Nassar G. Moazzami
Supervisory Patent Examiner

2/11/08